CLAIMS

What we claim is:

1. A communications security system to prevent transfer of selected communication transactions from an untrustworthy network to a trustworthy network, comprising:

a server, connected to the untrustworthy network, that maintains a database of protection rules, each of which, when applied to a communication transaction, identifies that communication transaction to be a respective one of the selected communication transactions; and

a portal, connected between the untrustworthy network and the trusted network, that:

selectively transfers the database of protection rules from said server via said untrustworthy network;

receives a communication transaction from the untrustworthy network for transfer to the trustworthy network;

applies each of the protection rules to the received communication transaction; and

prevents the transfer of the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions.

2. The security system of claim 1 wherein the transfer of the database from the server to the portal is via a secure protocol.

3. The security system of claim 1:

wherein each of said protection rules may be a selected one of two classes, exclusion or guard; and

wherein the portal:

prevents the transfer of the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions, if said protection rule is of the exclusion class; but

selectively transfers the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions, if said protection rule is of the guard class.

4. The security system of claim 3 wherein the portal selectively transfers to the server at least a portion of each received communication transaction identified to be a respective one of the selected communication transactions.

5. The security system of claim 4 wherein the server, in response to receiving said portion of a communication transaction identified to be a respective one of the selected communication transactions by a protection rule of the guard class, analyzes said portion to determine if said communication transaction represents a security threat to the trustworthy network, and, if it is so determined, constructs a new protection rule of the exclusion class and adds said new protection rule to said database.

6. The security system of claim 5 wherein the server analyzes said portion using an expert system.

7. The security system of claim 6 wherein the server constructs said new protection rule using the expert system.

8. The security system of claim 7 wherein the expert system is guided by a human expert.

9. The security system of claim 4 wherein the server, in response to receiving said portion of a communication transaction identified to be a respective one of the selected communication transactions by a protection rule of the guard class, provides said portion to a human expert to determine if said communication transaction represents a security threat to the trustworthy network, receives new protection rules from said human expert, and adds said new protection rules to said database.

10. A communications security method to prevent transfer of selected communication transactions from an untrustworthy network to a trustworthy network, comprising:

at a server, connected to the untrustworthy network, maintaining a database of protection rules, each of which, when applied to a communication transaction, identifies that communication transaction to be a respective one of the selected communication transactions; and

at a portal, connected between the untrustworthy network and the trusted network:

selectively transferring the database of protection rules from said server via said untrustworthy network;

receiving a communication transaction from the untrustworthy network for transfer to the trustworthy network;

applying each of the protection rules to the received communication transaction; and

preventing the transfer of the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions.

11. The security method of claim 10 wherein the transfer of the database from the server to the portal is via a secure protocol.

12. The security method of claim 10:

wherein each of said protection rules may be a selected one of two classes, exclusion or guard; and

wherein, at the portal, the step of preventing is further characterized as:

preventing the transfer of the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions, if said protection rule is of the exclusion class; but

selectively transferring the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions, if said protection rule is of the guard class.

13. The security method of claim 12 further comprising, at the portal:

selectively transferring to the server at least a portion of each received communication transaction identified to be a respective one of the selected communication transactions.

14. The security method of claim 13 further comprising, at the server:

receiving said portions of said communication transactions identified to be a respective one of the selected communication transactions; and

in response to receiving said portion of a communication transaction identified to be a respective one of the selected communication transactions by a protection rule of the guard class, analyzing said portion to determine if said communication transaction represents a security threat to the trustworthy network, and, if it is so determined, constructing a new protection rule of the exclusion class and adding said new protection rule to said database.

15. The security method of claim 14 further including, at the server:

analyzing said portion using an expert system.

16. The security method of claim 15 wherein, at the server, the step of constructing the new protection rule is further characterized as:

constructing said new protection rule using the expert system.

17. The security method of claim 16 wherein, at the server, the expert system is guided by a human expert.

18. The security method of claim 13 further comprising, at the server:

receiving said portions of said communication transactions identified to be a respective one of the selected communication transactions; and

in response to receiving said portion of a communication transaction identified to be a respective one of the selected communication transactions by a protection rule of the guard class, providing said portion to a human expert to determine if said communication transaction represents a security threat to the trustworthy network, receiving new protection rules from said human expert, and adding said new protection rules to said database.

19. A portal for use in a communications security system to prevent transfer of selected communication transactions from an untrustworthy network to a trustworthy network, the security system including a server, connected to the untrustworthy network, that maintains a database of protection rules, each of which, when applied to a communication transaction, identifies that communication transaction to be a respective one of the selected communication transactions, the portal, when connected between the untrustworthy network and the trusted network:

selectively transferring the database of protection rules from said server via said untrustworthy network;

receiving a communication transaction from the untrustworthy network for transfer to the trustworthy network;

applying each of the protection rules to the received communication transaction; and

preventing the transfer of the received communication transaction to the trustworthy network if a protection rule identifies the received communication transaction to be a respective one of the selected communication transactions.

20. A server for use in a communications security system to prevent transfer of selected communication transactions from an untrustworthy network to a trustworthy network via a portal, the server, when connected to the untrustworthy network:

maintaining a database of protection rules, each of which, when applied to a communication transaction, identifies that communication transaction to be a respective one of the selected communication transactions; and

selectively transferring the database of protection rules via said untrustworthy network to said portal for application by said portal to each communication transaction received by said portal to prevent the transfer of the received communication transaction to the trustworthy network by the portal if a protection rule, when applied by the portal, identifies the received communication transaction to be a respective one of the selected communication transactions.